PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-016593
(43)Date of publication of application : 18.01.2002

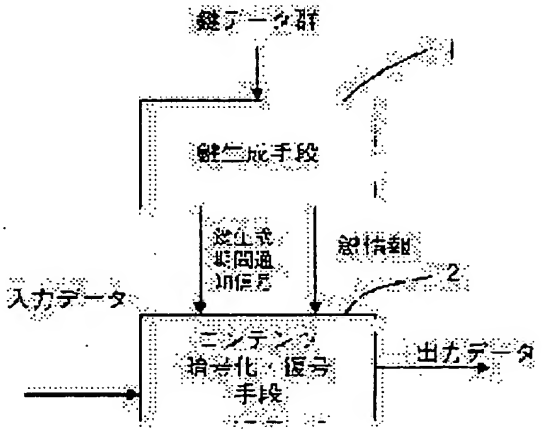
(51)Int.Cl. H04L 9/10
G06F 12/14
G06F 15/00
H04L 9/08
H04N 7/167
// G09C 1/00

(21)Application number : 2000-196080
(22)Date of filing : 29.06.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : OKAYAMA MUTSUYUKI
YANAGISAWA REIGO

(54) COPYRIGHT PROTECTION DEVICE AND COPYRIGHT PROTECTION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To solve the problem in the conventional copyright protection device that data have been obtained which differ greatly from the data obtained, when contents data are given to a contents encryption or decoding means and then outputted therefrom during generation of information used for encryption and decoding.
SOLUTION: While a key-generating means 1 generates key information used for encryption and decoding, the generating means 1 gives a signal denoting a key-generating state to a contents encryption decoding means 2 by means of a key-generating period notice signal, and the means 2 does not output data which result from encrypting or decoding contents. After generating the key information, the contents encryption decoding means 2 encrypts or decodes the contents and provides an output of the resulting data, on the basis of the key information received from the key information generating means 1.



LEGAL STATUS

[Date of request for examination] 08.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－16593
（P2002－16593A）
(43)公開日　平成14年１月18日(2002.1.18)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04L 9/10		G06F 12/14	320B	5B017
G06F 12/14	320	15/00	330A	5B085
15/00	330	G09C 1/00	660D	5C064
H04L 9/08		H04L 9/00	621Z	5J104
H04N 7/167			601D	

審査請求　未請求　請求項の数８　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願2000－196080(P2000－196080)

(22)出願日　平成12年６月29日(2000.6.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　岡山　睦之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

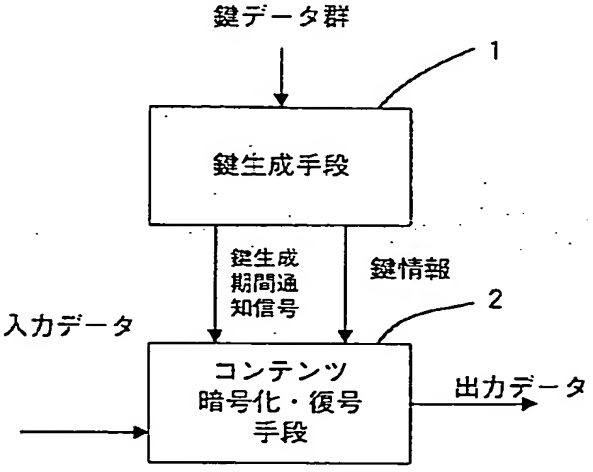
(72)発明者　柳澤　玲互
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　著作権保護装置および著作権保護方法

(57)【要約】
【課題】　情報を生成中にコンテンツのデータをコンテンツの暗号化もしくは暗号復号する手段に入力し、出力すれば、本来得られるべきデータと大きく異なったデータが得られてしまう。
【解決手段】　鍵生成手段１で暗号化および復号に使用する鍵情報を生成中は、コンテンツ暗号化・復号手段２に鍵生成期間通知信号で鍵生成中という信号を送り、その期間は、コンテンツの暗号化もしくは復号を行ってデータを出力しない。鍵情報を生成した後は、鍵情報生成手段１から送出された鍵情報をもとにコンテンツ暗号化・復号手段２でコンテンツの暗号化もしくは復号を行いデータを出力する。



1

【特許請求の範囲】

【請求項１】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力する鍵生成手段と、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵生成手段の出力である鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力するコンテンツ暗号化・復号手段とを備え、

前記コンテンツ暗号化・復号手段は、前記鍵生成手段の出力である鍵生成期間通知信号が鍵生成中と通知している場合には、コンテンツの暗号化もしくは復号を行った結果のデータを出力しないことを特徴とする著作権保護装置。

【請求項２】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力する鍵生成手段と、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵生成手段の出力である鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力するコンテンツ暗号化・復号手段と、

前記鍵生成手段の出力である鍵生成期間通知信号が鍵生成中と通知している場合には、前記コンテンツ暗号化・復号手段に入力されるコンテンツデータをそのまま出力し、前記鍵生成手段の出力である鍵生成期間通知信号が鍵生成中と通知していない場合には、前記コンテンツ暗号化・復号手段の出力データを出力する切替えスイッチ手段とを備えたことを特徴とする著作権保護装置。

【請求項３】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力する鍵生成手段と、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵生成手段の出力である鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力するコンテンツ暗号化・復号手段とを備え、

前記コンテンツ暗号化・復号手段は、前記鍵生成期間通知信号が鍵生成中と通知している場合はコンテンツデータの入力不許可信号を出力することを特徴とする著作権保護装置。

【請求項４】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力する鍵生成手段と、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵生成手段の出力である鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力するコンテンツ暗号化・復号手段とを備え、

前記鍵生成手段は、鍵生成中の時はコンテンツデータの入力不許可信号を出力することを特徴とする著作権保護装置。

【請求項５】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力し、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力する著作権保護方法であって、

前記鍵生成期間通知信号が鍵生成中と通知している場合には、コンテンツの暗号化もしくは復号を行った結果のデータを出力しないことを特徴とする著作権保護方法。

【請求項６】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力し、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力する著作権保護方法であって、

前記鍵生成期間通知信号が鍵生成中と通知している場合には、入力されたコンテンツデータをそのまま出力し、前記鍵生成期間通知信号が鍵生成中と通知していない場合には、暗号化もしくは復号した出力データを出力することを特徴とする著作権保護方法。

【請求項７】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力すると共に、鍵生成中は鍵生成期間通知信号を出力し、

コンテンツの暗号化もしくは復号を行うかどうかの識別信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力する著作権保護方法であって、

前記鍵生成期間通知信号が鍵生成中と通知している場合はコンテンツデータの入力不許可信号を出力することを特徴とする著作権保護方法。

【請求項８】コンテンツの暗号化もしくは復号を行うための鍵を生成して出力し、

コンテンツの暗号化もしくは復号を行うかどうかの識別

信号をコンテンツデータ内に有するコンテンツデータを入力し、前記識別信号を処理してコンテンツの暗号化もしくは復号を行うと判断した場合には、前記鍵を用いてコンテンツの暗号化もしくは復号を行ってデータを出力する著作権保護方法であって、
鍵生成中の時はコンテンツデータの入力不許可信号を出力することを特徴とする著作権保護方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は音声データや画像データ等のコンテンツの記録・再生・送信・受信を利用する装置に係るものであり、特にコンテンツの著作権を保護するための装置及び方法に関する。

【０００２】

【従来の技術】従来、アナログデータでは、音声データや画像データ等のコンテンツに対して、記録・再生・送信・受信等を行えば、品質が劣化するため、著作権の保護という観点では、大きな問題とならなかった。しかしながら、近年、ディジタル化がいっそう進み、音声データや画像データを初めとして、様々なコンテンツがディジタルデータ化されている。このようなディジタルデータに対しては、記録・再生・送信・受信等を行っても、品質劣化が殆ど生じないため、著作権の保護という観点で大きな問題が生じてきた。

【０００３】この問題を解決するために、様々な著作権保護技術が開発され、実用化にいたっている。その一つは暗号化の技術であり、例えば、DES暗号やRSA暗号等が知られている。暗号手法の詳細は、「現代暗号理論入門」電子情報通信学会編　池野信一　他　1998年11月出版に掲載されているので、ここでは割愛する。また具体的な装置としては、特開平8-287014号公報に記載がある。

【０００４】

【発明が解決しようとする課題】一方、暗号化もしくは、暗号の復号を行うための鍵を生成することは、多大な時間を要する。例えば、DVDレコーディングやDVDオーディオで用いられているContent Protection for Recordable Media (CPRM) やContent Protection for Prerecorded Media(CPPM)では、鍵を生成するまでに、認証や検証を行って、中間鍵を生成するため、多大な時間を要する。従って、鍵の生成中に平行してコンテンツのデータをコンテンツの暗号化手段もしくはコンテンツの暗号の復号手段に入力しても、鍵の生成時間が間に合わず、正しい鍵でコンテンツの暗号化もしくは復号を行なえない場合が生じる。すなわち、鍵の生成中に、データがコンテンツの暗号化手段に入力されれば、コンテンツの暗号化手段は、本来得られるべきデータと大きく異なったデータを生成し、出力してしまう。また、鍵の生成中に、データがコンテンツの復号手段に入力されれば、コンテンツの復号手段は、正しいコンテンツデータを生成せず、不良なデータを生成して、出力してしまう。

【０００５】また、特開平11-126423号公報では、コンテンツ内にあるコピービットにより、コピー可能かどうかを判断する旨の記載がある。このコピービットを識別信号として使用し、コピー可能かどうかが判断できた時点でコンテンツをコンテンツの暗号化手段もしくはコンテンツの復号手段に入力をする。しかしながら、コンテンツの暗号化手段もしくはコンテンツの復号手段の内部にコンテンツの暗号化・暗号復号を行うかどうかの識別信号を検出する機能を保有している場合は、コンテンツの暗号化手段もしくはコンテンツの復号手段に、この識別信号を入力することができないため、コンテンツの暗号化もしくはコンテンツの復号データを出力することができないという点で大きな課題があった。

【０００６】本発明は上記課題に鑑み、鍵を生成しつつ、コンテンツの先頭部分を欠落させる事無く、正しい鍵でコンテンツを暗号化したデータもしくは復号したデータを出力することができる著作権保護装置およびその方法を提供するものである。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明に係る著作権保護装置は、鍵生成中に、コンテンツの暗号化もしくは復号を行った結果のデータを出力しないことを特徴としている。またその手法としては、鍵生成中は、コンテンツの暗号化・復号処理の結果の出力をしないこともしくはコンテンツの暗号化・復号処理に入力を許可しない構成としたことを特徴としている。

【０００８】複雑な高能率符号化が施されたコンテンツに部分的に暗号が施されてディスクに記録されているとする。そのディスクを再生する際、鍵生成中は、コンテンツの暗号化・復号処理を施したデータを出力させずにコンテンツの暗号化・復号処理の入力信号をそのまま出力させる手法が特に有効である。この場合、コンテンツの高能率符号化を復号するための情報が少しでも出力されることになり、最終的にコンテンツの出力が早くなる。また、コンテンツを暗号化してディスクに記録する場合は、コンテンツの暗号化・暗号復号処理にデータの入力を許可しないことが特に有効である。この場合、コンテンツの暗号化・暗号復号処理手段は、鍵生成中の正しくないデータを出力する事無くしかもコンテンツの先頭が途切れる事がなくなる。

【０００９】

【発明の実施の形態】以下、本発明に係る著作権保護装置の実施の形態について、図面に基づいて詳細に説明する。

【００１０】（実施の形態１）まず、本発明の実施の形態１に係る著作権保護装置について説明する。図１は本発明に係る著作権保護装置の構成を示すブロック図である。図１において、１は鍵生成手段、２はコンテンツ暗

号化・復号手段である。図５は鍵生成手段１の一例のブロック図である。図５において、１０１は中間鍵の処理手段、１０２は最終鍵の処理手段である。

【００１１】図１および図５を用いて、本発明の実施の形態の動作説明を行う。

【００１２】本実施の形態１を容易に理解するために、鍵の生成アルゴリズムとして、次のアルゴリズムを仮定する。仮定するアルゴリズムはCPRMである。なお、詳細は4C Entity が2000年4月に発行したContent Protection for Recordable Media Specification -introduction and Common Cryptographic Elements とContent Protection for Recordable Media Specification -DVD Bookを参照されたい。記録機器と記録媒体が存在する。ここで、記録機器はDVD記録再生機器もしくはDVDプレーヤを仮定する。また、記録媒体は、DVD記録再生ディスクもしくはDVD再生ディスクを仮定する。なお、本発明はこれらDVD機器に限定するものではないことは言うまでもない。そして、暗号を施すかどうかの識別信号はコンテンツ内に存在し、コンテンツ暗号化・復号手段２が識別信号を判断して処理を行う。DVD記録再生機器には、装置鍵として、装置鍵Ａが存在する。DVD記録再生ディスクには、媒体鍵と媒体認識子が存在する。ここで、媒体鍵は予め、装置鍵で暗号化された状態でディスクに書き込まれている。装置鍵は装置毎に異なるため、暗号化された媒体鍵は複数となる。これを暗号化された鍵データ群と称している。CPRMのアルゴリズムに従えば、装置鍵、媒体鍵の他に、媒体鍵と媒体認識子で演算を施して得られる媒体独自鍵、乱数の発生により得られる表題鍵と表題鍵に対して、ストリームデータで演算を施して得られる内容鍵がある。また、表題鍵は媒体独自鍵で暗号化して、ディスクに記録される。再生時には、暗号化された表題鍵を媒体独自鍵で復号する。詳細は上記にあげた参考文献に示されているので、そちらを参照されたい。ここでは、装置鍵として装置鍵Ａ、媒体鍵として媒体鍵Ａ、媒体独自鍵として媒体独自鍵Ａ、表題鍵として表題鍵Ａ、内容鍵として内容鍵Ａを設定する。そして、装置鍵Ａで媒体鍵Ａを暗号化して、ディスクに記録してある。

【００１３】DVD記録再生装置にディスクを挿入して、コンテンツを再生する場合を想定する。鍵生成のスタートとして、暗号化された媒体鍵Ａが暗号化された鍵データ群として、鍵生成手段１に入力される。装置鍵Ａは何らかの形で既に鍵生成手段Ａに入力されている。例えば、予め固定的に入力されていても良いし、ある種の変換された形で外部から入力し、鍵生成手段１で元に戻して、装置鍵Ａを得ても良い。そして、媒体認証子を鍵生成手段１に入力して、媒体鍵Ａを媒体独自鍵Ａに変換する。さらに、暗号化された表題鍵を鍵生成手段１に入力して、媒体独自鍵Ａを表題鍵Ａに変換する。この鍵生成手順をもう一度図５を用いて説明する。装置鍵Ａが図５における鍵情報である。これに対して、暗号化された媒体鍵Ａが暗号化された中間鍵である。中間鍵処理手段１０１により、鍵情報を用いて、暗号化された中間鍵を復号して、中間鍵Ａを得る。これが媒体鍵Ａとなる。さらに、媒体認証子を暗号化された中間鍵として、入力し、すでに得られている媒体鍵Ａに対して、変換を行い、新たな中間鍵を得る。これが、媒体独自鍵Ａとなる。そして、暗号化された最終鍵として、暗号化された表題鍵を入力すれば、最終鍵処理手段１０２により、中間鍵を用いて、復号処理を行い最終鍵を得る。これが、表題鍵Ａとなる。

【００１４】この表題鍵Ａがコンテンツ暗号化・復号手段２に入力される。コンテンツ暗号化・復号手段２では、コンテンツが暗号化された暗号文データが入力される。そして、この暗号文データ中の一部の情報を用いて、表題鍵Ａを内容鍵Ａに変換する。暗号化もしくは復号を行うかどうかは、コンテンツ内にある識別信号を見て、コンテンツ暗号化・復号手段２が判断する。識別信号を見て判断した結果、復号を行う場合には、この内容鍵Ａにより、暗号文データの復号が行われ、平文データのコンテンツが出力される。

【００１５】ここで、装置鍵Ａもしくは媒体鍵Ａなどの中間鍵が生成開始から媒体独自鍵Ａなどの中間鍵もしくは表題鍵Ａなどの最終鍵の生成完了までの期間を鍵生成期間通知信号として、コンテンツ暗号化・復号手段２に出力する。コンテンツ暗号化・復号手段２は鍵生成期間通知信号がアクティブの場合、すなわち、鍵生成期間中の場合には、出力データを出力しない。

【００１６】以上により、正しくない鍵で暗号化もしくは復号を行った結果のデータを出力しないので、次段の処理手段に悪影響を及ぼさない。

【００１７】なお、本実施の形態では、暗号化されたコンテンツの復号であったが、逆に平文データのコンテンツを暗号化する場合でも良い。さらに鍵生成アルゴリズムとして、媒体独自鍵Ａ、内容鍵Ａは共に無くても良いし、片方のみあっても良い。さらに、表題鍵Ａを生成する過程がさらに複雑であっても良い。

【００１８】（実施の形態２）次に、本発明の実施の形態２に係る著作権保護装置について図４、図５及び図６を用いて説明する。図４は本実施の形態２の著作権保護装置の構成を示すブロック図である。図４において、１は鍵生成手段、２はコンテンツ暗号化・復号手段、３は出力信号切替えスイッチである。図５は鍵生成手段２のブロック図であり、実施の形態１と同等のものである。図６は本発明の実施の形態２における入力信号のタイミングチャートである。本発明の実施の形態２が実施の形態１と異なる所は、鍵生成期間通知信号により、コンテンツ暗号化・暗号復号手段２からの出力データかコンテンツ暗号化・暗号復号手段２への入力データかのいずれかを選択して、出力する点である。鍵の生成過程は実施の

形態１と同等であるので、ここでは割愛する。さらに、コンテンツ暗号化・復号手段２の動作も同等であるので、ここでは割愛する。出力信号切替えスイッチ３の動作が異なるので、出力信号切替えスイッチ３の動作のみを図６を用いて説明する。

【００１９】出力信号切替えスイッチ３は鍵生成手段１の出力信号である鍵生成期間通知信号が非アクティブの場合、即ち、鍵生成期間中で無い場合、コンテンツ暗号化・復号手段２の出力信号を選択し、外部に出力する（図６中、切替えスイッチの出力が0*（*は数字）“００”、“０１”等）。そして、出力信号切替えスイッチ３は鍵生成手段１の出力信号である鍵生成期間通知信号がアクティブの場合、すなわち、鍵生成中の場合、コンテンツ暗号化・復号手段２の入力信号を選択し、そのまま外部に出力する（図６中、切替えスイッチの出力がＤ*（*は数字）“Ｄ０”、“Ｄ１”等）。

【００２０】以上により、正しくない鍵で暗号化もしくは暗号復号を行った結果を出力しないので、次段の処理手段に悪影響を及ぼさない。

【００２１】（実施の形態３）次に、本発明の実施の形態３に係る著作権保護装置について図２、図５及び図７を用いて、本発明の実施の形態３を説明する。図２は本発明の実施の形態３の著作権保護装置の構成を示すブロック図である。

【００２２】図２において、１は鍵生成手段、１１はコンテンツ暗号化・復号手段である。図５は鍵生成手段１のブロック図であり、実施の形態１と同等のものである。図７は本実施の形態３における入力信号のタイミングチャートである。本発明の実施の形態３が実施の形態１および実施の形態２と異なる所は、鍵生成期間通知信号がアクティブの時、すなわち、鍵生成期間中の場合、コンテンツ暗号化・復号手段２へのデータ入力を許可しないように、コンテンツ暗号化・復号手段２の出力信号である入力許可信号を非アクティブにする点である。

【００２３】鍵の生成過程は実施の形態１と同等であるので、ここでは割愛する。さらに、コンテンツ暗号化・復号手段１１の動作のうち、コンテンツの暗号化・復号動作も同等であるのでここでは割愛する。コンテンツ暗号化・復号手段１１の動作のうち入力許可信号の出力が異なるので、その動作のみを図７を用いて説明する。鍵生成手段１から出力される鍵生成期間通知信号がアクティブの時、コンテンツ暗号化・復号手段２は入力許可信号を非アクティブにして、出力する（図７中、入力許可信号=“Ｌ”レベルの時）。また、鍵生成手段１から出力される鍵生成期間通知信号が非アクティブの時、コンテンツ暗号化・復号手段２はコンテンツ暗号化・復号手段２が入力信号を受け入れ可能かどうかを判断して、入力信号を受け入れ可能であれば、入力許可信号をアクティブにして出力（図７中、入力許可信号=“Ｈ”レベルの時）し、入力信号を受け入れ不可能であれば、入力許可信号を非アクティブにして出力する。

【００２４】以上により、鍵情報生成中の正しくないデータを出力する事が無い。

【００２５】（実施の形態４）次に、本発明の実施の形態４に係る著作権保護装置について図３および図５を用いて説明する。図３は本発明の実施の形態４の著作権保護装置の構成を示すブロック図である。図３において、１０は鍵生成手段、２はコンテンツ暗号化・復号手段である。図５は鍵生成手段の鍵生成部のブロック図であり、実施の形態１と同等のものである。本発明の実施の形態４が実施の形態３と異なるところは、入力許可信号の出力がコンテンツ暗号化・復号手段２ではなく、鍵生成手段１０から出力される点である。

【００２６】鍵生成過程およびコンテンツ暗号化・復号手段の動作は本実施の形態１と同等であるので、ここでは割愛する。鍵生成手段１０が入力許可信号を出力する動作が異なるのでその動作のみ説明する。鍵生成手段１では本実施の形態３と同等の鍵生成期間通知信号が生成される。この鍵生成期間通知信号がアクティブの時、すなわち、鍵生成期間中の時には、入力許可信号が非アクティブで出力される。また、鍵生成期間通知信号が非アクティブの時、すなわち鍵生成期間中でない時には、入力許可信号がアクティブで出力される。

【００２７】以上により、鍵情報生成中の正しくないデータを出力する事が無い。

【００２８】

【発明の効果】以上説明したように、本発明の著作権保護装置によれば鍵情報を生成中は、復号化データ、暗号化データを出力しないので、誤ったデータを出力しない。

【００２９】また、ディスクを再生する際、鍵生成中は、コンテンツの暗号化・復号処理を施したデータを出力させずにコンテンツの暗号化・復号処理の入力信号をそのまま出力させる方法を利用する場合、コンテンツの高能率符号化を復号するめの情報が少しでも出力されることになり、最終的にコンテンツの出力が早くなる。

【００３０】また、コンテンツを暗号化してディスクに記録する場合は、コンテンツの暗号化・暗号復号処理にデータの入力を許可しない方法を利用すると、コンテンツの暗号化・暗号復号処理手段は、鍵生成中の正しくないデータを出力する事無くしかもコンテンツの先頭が途切れる事がなくなる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係る著作権保護装置の信号処理ブロック図

【図２】本発明の実施の形態３に係る著作権保護装置の信号処理ブロック図

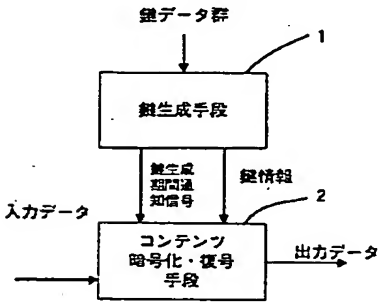
【図３】本発明の実施の形態４に係る著作権保護装置の信号処理ブロック図

【図４】本発明の実施の形態２に係る著作権保護装置の

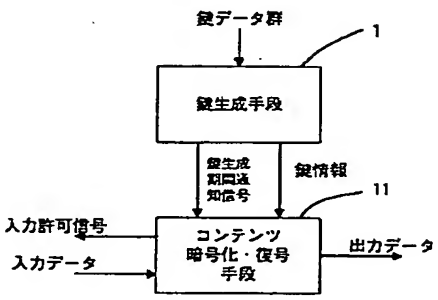
信号処理ブロック図
【図５】本発明に係る著作権保護装置の鍵情報生成ブロック図
【図６】本発明の実施の形態２に係る著作権保護装置の入力信号のタイミングチャート
【図７】本発明の実施の形態３に係る著作権保護装置の入力信号のタイミングチャート
【符号の説明】

１　鍵生成手段
２　コンテンツ暗号化・復号手段
３　切替えスイッチ
１０　鍵生成手段
１１　コンテンツ暗号化・復号手段
１０１　中間鍵の処理
１０２　最終鍵の処理

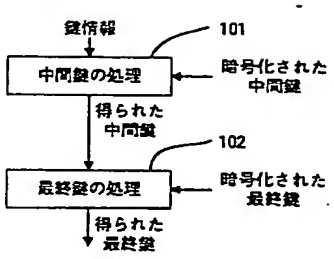
【図１】



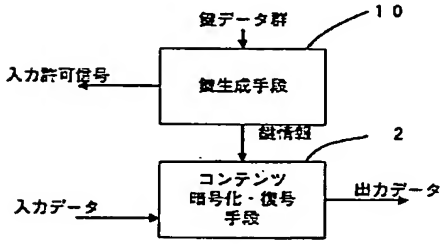
【図２】



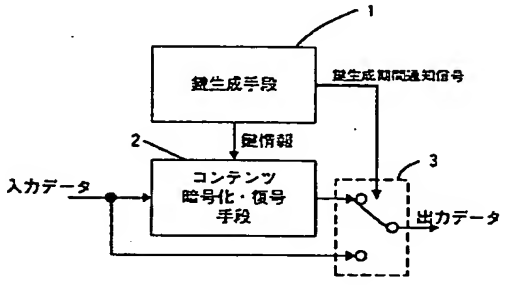
【図５】



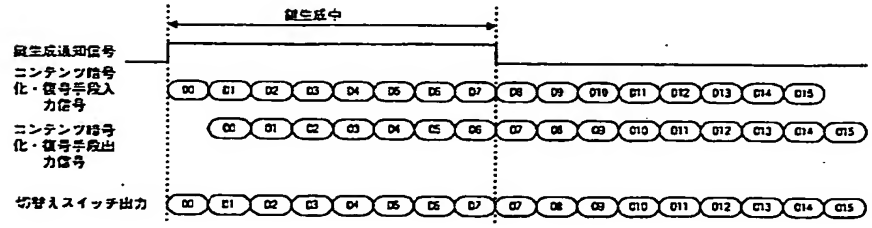
【図３】



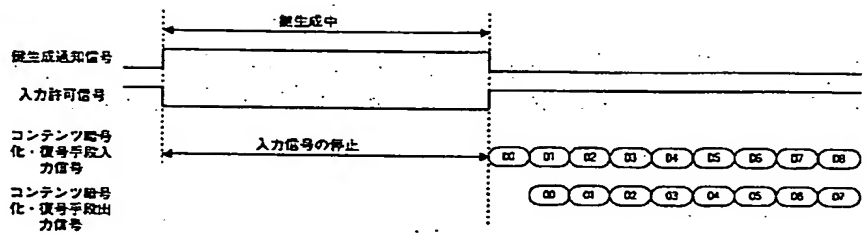
【図４】



【図６】



【図７】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
// Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｎ　7/167	Ｚ	

Ｆターム(参考)　5B017 AA03 AA08 BA07 CA16
5B085 AA08 AE29
5C064 CA14 CB01 CC02 CC04
5J104 AA12 AA32 EA04 EA17 EA23
NA02 NA03